CONTENTS

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker

VOL. 4 NO. 8 AUGUST 1987 $2

DO YOU HAVE BACK ISSUES OF *2600*? If not, look what you're missing!

1984

AHOY!—an introduction to 2600; FBI GOES AFTER ADS HACKERS—FBI investigator unwittingly reveals tactics and recent activities; FLASH: LICA discusses GTE raids, AT&T credit cards, wireless phone trouble; THE TRUTH BEHIND THOSE 9999 NUMBERS—a toll-free error story; DATA: various White House extensions; HACKING ON TELENET—how to use Telenet; ESS: ORWELL'S PROPHECY—the first in a series on the fun and dangers of ESS; FLASH: directory assistance changes, computer air-burn, AT&T credit cards, etc.; SOME THOUGHTS ON GARBAGE PICKING—first of a series on trashing for valuable information as related to a discussion of crosstalk; DATA: COUNTRY CODES—every last country code for overseas dialing; THE CONSTITUTION OF A HACKER—a discussion of hacking; ALTERNATE LONG DISTANCE: MCI—history, systems, and services; FLASH: 718, Connecticut wiretaps, Sweden person numbers, etc.; THE FIRST ATOMIC BOMB—an inside story on the event as related to our nation's phone system; DATA: ARPANET HOSTS—list of accessible hosts; WHOSE STRIKE WAS THAT ANYWAY?—a startling analysis of summer 83 phone strike; THE TROUBLE WITH TELEMAIL—discussion of GTE's irresponsibility in protecting their system; FLASH: AT&T credit cards, portable prisons, 414's plead, etc.; A TRUE SAGA OF TELECONFERENCING—what can happen on a teleconference; DATA: MCI ACCESS NUMBERS—DIAL UPS FOR MCI MAIL; PHONE BOOK COLLAGE #1—our artistic heritage in phone book designs; THE SIMPLE PLEASURES OF A STEP OFFICE—discussion of the ins and outs of antiquated phone systems; IBM'S AUDIO DISTRIBUTION SYSTEM—using voice messaging technology; FLASH: 414 sentencing, equal access, bank record privacy, etc.; THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY—a true story; DATA: AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK—a list including base addresses; EASYLINK ACCESS NUMBERS; ARPANET HOPPING: AMERICA'S NEWEST PASTIME—how it works and tips for its use; ELECTRONIC SWITCHING ADVANCES—some of the possible services and drawbacks; FLASH: Directory assistance changes, 2600 writer indicted, demise of E-COM, etc.; THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP—a frank discussion; LETTERS: sysop problems, 618 789 an XY step, etc.; DATA: E-COM ACCESS NUMBERS—dial ups for the (now defunct) service; NY TELEPHONE "LETTER OF DOOM"—a copy of a law-enforcement monitoring notice; "LOOK OUT, HE'S GOT A COMPUTER!"—a defense of the hacker viewpoint; MCI MAIL: THE ADVENTURE CONTINUES—an analysis of the well known faulty E-mail system; FLASH: computerized never-mad, blue box arrests, anti-hack legislation; INTRODUCING THE CLEAR BOX—"post pay" payphone device; LETTERS: new switching equipment, 99 scanning, repulsive operator story, etc.; SPECIAL REPORT: TRW—BIG BUSINESS IS WATCHING YOU—how to use TRW, and an assessment of the potential of this system; BUT HOW DOES IT WORK?—a simple explanation of the phone system, ringing voltages, black boxes, etc.; PRIVACY LOST—a review of David Burnham's book "The Rise of the Computer State"; BE NICE TO YOUR TELCO—how individuals are abusing their telcos; FLASH: Big Brother in Miami, NASA computer break-in, computer export controls, 800 directories; LETTERS: phone sound-alikes, page numbers, hacker's book, etc.; DATA: CNA NUMBERS—list of CNA's; A HACKER'S GUIDE TO AN AREA CODE—a simple scheme to help "map out" exchanges in your area; HISTORY OF BRITISH PHREAKING—an account of the history and techniques; MORE ON TRASHING—what to look for, where to go, how to act; A FRIEND IN HIGH PLACES—story of a friendly operator; FLASH: NSA insecurity, hacker caught, private directories; LETTERS: phone bugs, WATS, TAP, etc.; DATA: A NON-COPYRIGHTED DIRECTORY; NY TELEPHONE "BIG BROTHER"; LETTERS—touch tone without permission, etc.; GETTING CAUGHT: HACKER'S VIEW—a story of the personal effects of hacking; VITAL INGREDIENTS—what makes the phones work: operators, switching; FLASH: NSA wants better phones, crime-computer victim, wiretap loopholes, 911 [illegible]; LETTERS: BBS discussion, Consent Letter, Computer Crime Data, others; DATA: NY TELEPHONE SECURITY NUMBERS; MCI ANECDOTE—bits, vulgarisms, MCI chairman profile; PHONE BOOK COLLAGE #2; EXPLORING CAVES IN TRAVELNET—an interesting extender explained; FUN WITH FORTRESS FONES—what a pay phone does, how people beat them; FLASH: SS computer fault, [illegible]; LETTERS: book list, silver boxing, another hacker's view; DATA: ICS AND CARRIER IDENTIFICATION CODES—guide to 950 exchange; MCI MAIL: TROUBLE LETTERS—the harassment begins; A TIME FOR REFLECTION—the year in review; MCI MAIL AND EASYLINK—electronic mail; THE SCARIEST NUMBER IN THE WORLD—true story; FLASH: campaign computer, [illegible] by phone, students bug computer, electronic call, federal phone upgrade; SURVEY—reader survey responses; SOME, BUT NOT ALL, ELECTRONIC MAIL SYSTEMS—list and price comparisons plus voice messaging companies; REACH OUT AND GOOSE SOMEONE—list of many unique dial-it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN—analysis of Newsweek incident; WIRETAPPING AND DIVESTITURE—a lineman discusses these topics; GETTING IN THE BACK DOOR—a guide to some popular operating systems including TOPS 10, TOPS 20, and UNIX; 2600 INFORMATION BUREAU: our phone bill, our thanks, and other notices; FLASH: IRS and telco data, GEISCO, KKK computer; LETTERS: BBS rights, Easylink, Canada loops, international phreak day; BITNET TOPOLOGY—a schematic of the Bitnet; THE THEORY OF "BLUE BOXING"—history, future, and how they are used; TRASHING ALASKA STYLE—a real trashing adventure story; SURVEYING THE COSMOS—a beginner's guide to COSMOS, Bell's computer program; FLASH: phreak roundups, real TRW crime, 2600 BBS, 900 dial; LETTERS: Bell problems, telco discount, marine calling, many questions; 2600 INFORMATION BUREAU—acronym list of useful telephone jargon; NAZI BBS A CHALLENGE TO HACKERS—the role of the hacker; ARE YOU A PHREAK???—humourous review of phreaking; HOW TO GET INTO A C.O.—a tour of a central office; FLASH: custom calling, Kenyan pay phones, hacker coke machine, IRS computer screw-up; LETTERS: reading list, tracing and law enforcement, UNIX info, NSA phone #; 2600 INFORMATION BUREAU—interesting phone numbers, how to dial a telephone, New York Tel message; CNA LIST; NSA CIPHER DISK; WHAT A WHITE BOX CAN DO—how to build and the use of a portable touch tone generator; A PHONE PHREAK SCORES—another successful social engineering story; HACKING PACKARD—useful information about the HP2000; FLASH: talking clock, computers for communists, robot kills man, war games, silver pages; LETTERS: Tom Tompkins, secure telephones and cryptography; 2600 INFORMATION BUREAU—MILNET hosts by location; PEOPLE EXPRESS TO BE HACKED TO PIECES—a look at People's new anonymous reservation service; HOW TO RUN A SUCCESSFUL TELECONFERENCE—complete guide to Alliance Teleconferencing Service; FLASH: hacker bust, police hacker, Reagan doesn't dial kids, dial a directory; LETTERS: computer networks, silver boxes, 950 remote tracing; 2600 INFORMATION BUREAU—All new Teleconferencing material; INTERESTING PHONE NUMBERS; UNBELIEVABLE ADVERTISEMENT; GUIDE TO THE ISRAELI PHONE SYSTEM; SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE; SOME WORDS ON HACKER MORALITY; OUT OF THE INNER CIRCLE REVIEWED—an ex-hacker's new book; FLASH: who invented the phone, porno phone, wiretap award, AT&T computer steals; LETTERS: information charges, AT&T cutoff, marine calling; 2600 INFORMATION BUREAU—800 prefixes by state; SYSTEMATICALLY SPEAKING—goodbye to meter readers, free phone books, tracking devices, TINA, "Call Me" Card; FROM SHERWOOD FOREST: INTRO TO HACKING—what to do and not to do; INTERESTING THINGS TO DO ON A DEC-20—how to use various commands and some things to look for; BANKING FROM YOUR TERMINAL: A LOOK AT PRONTO—Electronic banking: how it works with a focus on Chemical's system; FLASH: $2 billion error, ITT crackdown, monitoring; 2600 INFORMATION BUREAU—Mitres TAC dialups by location; SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T; SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS—an accurate account of the Private Sector BBS; COMMENTARY: THE THREAT TO US ALL—what BBS seizures mean; FLASH: 2600 a hacking victim, Middlesex Courthouse, MOVING SATELLITES: WHAT WAS REALLY GOING ON?—point by point correction of New Jersey prosecutors' fallacious charges; WHY COMPUTERS GET SNATCHED—why law enforcement seizes equipment; SOME IMPORTANT QUESTIONS TO ASK—provocative questions about these events; HOW CAN SYSOPS PROTECT THEMSELVES?; A GUIDE TO VMS—how to use DEC's VAX operating system; THE INFINITY TRANSMITTER—an old bug explained; REACHING OUT ON YOUR OWN—blue boxing via fiction; PURSUIT FOR PEOPLE—GTE Telenet's computer to computer line up service; FLASH: phone-in registration, 800 word numbers, war game addict, hacker entertainer; 2600 INFORMATION BUREAU—Telenet directory of interesting addresses; SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, surveillance standardizing telcoms; MANY FAMILIAR TONES, AND THEY CALL US CROOKS!—story of a phone phreak who can't sell the phone tree; AN INTERESTING DIVERSION—call diverters and how they are abused; MORE INFO ON VMS—second installment of an in-depth guide to VMS; FLASH: computer elections, big phone bill, Navy phreaks, phone booth captures man; LETTERS: BBS suggestion, colleges are a gold mine, recommended reading; 2600 INFORMATION BUREAU—Blue Box plans; THE NEW AT&T HOSTAGE PHONE—unbelievable ad; SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, directions woes; RSTS: A TRICK OR TWO—some aspects of this operating system; THE SECRET REVEALED—the problem with GTE's GTD-5 switch; HISTORY OF ESS; EQUAL ACCESS MAY NOT BE "EQUAL" TO MODEMS—some problems that may arise; FLASH: columnists attack AT&T, feds don't it too much, little town phones, Springsteen mania; LETTERS: some advice, CIC's and free calls, British phreak, blue boxing gone?; CHASE BANK IS CRACKED; 2600 INFORMATION BUREAU—more interesting test numbers; SYSTEMATICALLY SPEAKING: AT&T to reduce mail; OUR WISHES FOR '86 AND BEYOND—some of what we'd like to see in the future; FUN WITH COSMOS—how to interpret and use parts of the phone company computers; FLASH: French phones, racist banter, Cryphone; SURVEY—reader survey responses; 2600 INFORMATION BUREAU—BBS numbers; SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super payphone.

(continued on inside back cover)

The Summer Games of 87

We've seen this so many times before. Nationwide raids of computer equipment at teenagers' houses. Newspaper headlines about electronic gangsters. Long periods of silence from the investigators and the investigated.

First the facts: at least six homes across the country were raided by the Secret Service in mid-July. They were in Rockville, Maryland; Burlingame, California; Kentfield, California; two in Brooklyn, New York; and one in Bronxville, New York. (At the same time, a number of houses in Pittsburgh were being searched, supposedly for simple credit card fraud and reportedly unrelated to the action that we are concerned with.)

What were these people allegedly up to? Everyone seems to want a piece of this one. Los Alamos National Laboratories, Stanford University, TRW, US Sprint, AT&T, MCI, and local phone companies are the ones we've heard from so far.

Unfortunately, when something like this occurs and very little additional information is given out, imaginations

(continued on page 5)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Managers
Fran Westbrook
Peter Kang

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
For letters and article submissions, write to: *2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0752.
Telephone: (516) 751-2600

TRW Credentials Lack Credibility

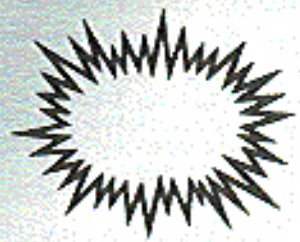
by Rex Valve

One of the powers commonly attributed to the modern American hacker is absolute control over the credit ratings of those who oppose them. Like all myths, this one too has a factual basis, which is probably the well-publicized invasions of the TRW credit service, documented in the 1984 editions of *2600*. Hacker visitations to TRW received widespread media coverage when *Newsweek* columnist Richard Sandza found his credit card numbers and similar private information posted on a hackers' bulletin board. Subsequent investigation revealed that due to TRW's shoddy security practices, hackers had the ability to make inquiries into TRW's vast database of American consumers' credit histories.

Now TRW is offering to those same American consumers the ability to look at their own credit reports, and to see who makes inquiries. Their new service, called TRW Credentials, lets a credit user look at his or her credit report, receive a notification whenever anyone else gets a copy of it (such as a bank where an application for a credit card or loan is pending) and the ability to add information that may improve one's credit rating. Anyone with or without a credit history can subscribe, as long as they're willing to fork over $35 a year.

However, a closer look at their service reveals that they are only selling a more convenient (and expensive) version of what they must already provide to you under the law. The Fair Credit Reporting Act requires that companies who compile credit histories make their information available to the individuals in question, if they request it. For an $8 fee (the minimal charge permitted under the act), they will send you your credit file. The file will include a list of all institutions who have received copies of it during the past year. If you find something in your file that is incorrect, you can protest to TRW, who will then investigate by asking the institution who provided the contested datum to verify its accuracy. This applies to any credit history service, not just TRW. Another feature of the Act is that if you are denied credit, such as being refused for a loan or credit card, you can (within 10 days) request a copy of your credit file without needing to pay the fee.

Well, this is America, and there's nothing wrong with companies trying to sell you something that you should already have. To make it look like you're buying more than the Fair Credit Reporting Act, TRW adds on a "Financial Profile" form, which supposedly lets you add information to your credit file that may improve your chances at getting credit. But there's nothing you can put on this form that can't be put on an ordinary loan application, and the subscribing credit grantors (such as banks or department stores that also subscribe to TRW Credentials) that might look at this information receive it on a separate form. It turns out that all TRW is saving you is the trouble of filling out a credit application all the way. On top of this they throw in insurance against unauthorized use of your cards (which the law already protects you against, beyond the first $50), and the ability to send your credit report to credit grantors elsewhere in your state, should you want to shop around for a loan (but only if you live in California or New York, and only with credit grantors who already subscribe to TRW Credentials). All in all, a dubious value.



The Summer Games of 1987

(continued from page 3

tend to roam wild. Given the overall technological illiteracy of the media and law enforcement coupled with the almost hysterical paranoia of the phone phreaks and computer hackers, it soon becomes abundantly clear that nobody knows what the hell is going on.

That's what's most disturbing here. It's one thing to break into people's homes and go on a confiscating binge if you've got something to say when others ask why. To do otherwise is not too far from arresting someone and holding them without naming a specific crime. Having most of your possessions taken away from you is unsettling enough without having to wait to find out why.

We also have many questions concerning the methods used. A teenager was almost shot by the Secret Service when he reached for a shirt after having been woken up in his room. Naturally, they assumed he was reaching for a gun—that's what hardened criminals are supposed to do, after all. A member of AT&T security found this out—from the Secret Service themselves. Apparently they thought it was funny.

The Secret Service knocked down at least two front doors with battering rams in their haste to get into these homes. In each case that we heard of, there was substantial damage, much more than what was necessary to get in. That according to neighbors and eyewitnesses.

And in at least one other instance, the Secret Service disguised themselves as United Parcel Service employees. They had a truck, packages, even the standard UPS clipboard.

We've had other reports of agents who refused to identify themselves, didn't produce search warrants, or acted in a rude fashion.

What in the world is going on here? Are these atrocities to be tolerated? Is the Secret Service attempting to live up to their initials or are they just incredibly unaware of what they're really doing?

These were all teenagers who were involved in the raids. And while they may have been quite intelligent, they most certainly were not about to shoot at police or pose any kind of a threat. There was no need to "trick" them into opening the door. That kind of gimmick is appropriate for mobsters perhaps, but not for adolescents.

We object to the methods used by the Secret Service. In fact, we question the very use of the Secret Service themselves. Why was a group such as this called in to deal with a matter that virtually any law enforcement entity could have handled?

Regardless of what comes out of this case (if one is ever even presented), the events that transpired are quite inexcusable. Unfortunately, most of those involved have been scared into silence. Scared by the strongarm tactics of the law, scared by the sensationalist media, scared by not knowing what the hell is going on. This is a very scary situation.

If such an occurrence should happen to you or anyone you know, this is what we suggest: Keep an eye on everything that is going on. Remember what is taken, what is handled, what is said. Write it all down when they leave. Do not, under any circumstance, give them an excuse to play rough. Law enforcement types can take lives and they can often get away with it. You don't have to answer any questions without a lawyer present. Get the names of everyone who comes into your house—you are most certainly entitled to know this. And if you do decide to talk to the media, avoid the sensationalist types like The New York Post. Go for the newspapers that put a little time into their stories and have been known to uncover things in the past. Make sure they understand what

(continued on page 14)

numbers of interest

201 221 3778 AT&T
201 480 1368 BCS
201 544 2062 FORT MONMOUTH
201 544 2072 FORT MONMOUTH
201 544 2784 FORT MONMOUTH
201 544 2812 FORT MONMOUTH
201 544 2915 FORT MONMOUTH
201 544 2946 FORT MONMOUTH
201 724 6731 DOVER
201 724 6732 DOVER
201 724 6733 DOVER
201 724 6734 DOVER
201 885 1242 AT&T
201 885 5111 AT&T
201 885 9540 AT&T
202 227 3526 BETHESDA
202 334 6831 WASHINGTON POST
202 347 3222 FAA
202 429 6700 DIAL TONE
202 553 0229 PENTAGON
202 633 7553 DEPT OF TREASURY
202 653 1079 NAVY
202 694 0004 PENTAGON
202 695 5261 CASPAR WEINBERGER
202 697 0814 PENTAGON
202 728 0124 US SPRINT
205 279 9575 SUMTER AFB
205 852 0926
207 876 3317
208 852 3072
213 826 6272
213 944 4523 STOCKTON SCHOOL
212 242 0023 NYC GEN SER
212 315 4078
212 369 5114 SPENCE
212 502 5694
212 520 7719 QUEENS COLLEGE
212 536 0587 NYC BOARD OF ED
212 598 7093 COLLEGE
212 735 3277 RAPID DATA
212 769 1996 BUDDY SYSTEM
212 769 1997 BUDDY SYSTEM
212 769 1998 BUDDY SYSTEM
212 777 7609 COLLEGE
212 777 7880 NYU
212 922 9387 ISRAEL/HOLLAND TONES
212 922 9393 VENEZ/S.AFRICA TONES
212 947 7522
213 204 4670 TDD
213 370 0787
213 379 0909 TDD
213 383 7073 FAX
213 417 8394 TWX
213 499 4040 CALTECH
213 581 4545
213 642 2706 LOYOLA COLLEGE
213 643 2690 ED SEGUNDO AFB
213 687 4562 CALTECH
213 772 6747
213 798 2000 FTS (FEDERAL TEL)
214 235 8729
214 263 3103 NAZI BBS
214 331 4043
214 742 1354 SOUTHWESTERN BELL
214 742 1537 SOUTHWESTERN BELL
214 742 2636 NTRCHA
214 954 9858 JOKES
215 253 7203
215 284 9010 GENERAL ELECTRIC
215 295 9513
215 563 9213 AF 2009
215 654 7139
215 949 3761
216 741 9912
216 995 3332 AMERITRUST
217 424 3450 SCHOOL DISTRICT #61
219 435 7722
219 932 6067
301 278 3916 ABERDEN PROVING GNDS
301 656 4700
301 728 5005
301 863 4815 PATUXENT RIVER
301 863 4816 PATUXENT RIVER
303 232 8055 HP 3000
303 284 5130
303 371 1236 JC PENNEYS
303 447 2540 COCIS
303 499 7111 BUREAU OF STANDARDS
303 522 2144 LIBRARY
303 753 2733 DENVER UNIVERSITY
303 753 2737 DENVER UNIVERSITY
303 770 9563
303 778 8860
303 978 8111 WANG VSC 80
304 376 2488 SEATTLE SAVINGS
304 927 1773 NAZI BBS
305 592 3148
305 851 5127 AT&T
305 851 7406 AT&T
309 344 9156 NASA
312 222 1911 CHICAGO TRIBUNE
312 250 5534 AT&T
312 253 9789 NAZI BBS
312 254 3919 CHICAGO EDUCATION
312 286 0282 ILLINOIS BELL
312 352 7000 TIMESHARING
312 393 5918 FERMILAB
312 396 6170 ILLINOIS SCHOOL
312 398 8170 SCHOOL DISTRICT #214
312 417 8394 TWX
312 432 1867 HIGHLAND NATIONAL
312 432 9401 COSMOS
312 470 8552 HIGH SCHOOL
312 492 3094 NORTHWESTERN
312 530 1755 COSMOS
312 567 5700 ITT
312 567 6478 ITT
312 567 6479 ITT
312 567 6480 ITT
312 567 6494 ITT
312 567 6890 ITT
312 567 6993 ITT
312 567 6896 ITT
312 592 6230 CONFERENCE BRIDGE
312 592 6231 CONFERENCE BRIDGE
312 640 5750 DIGITAL COMPUTERS
312 671 3013 PBX
312 671 3214 PBX
312 671 7505 PBX
312 673 9091
312 686 0697 O'HARE AIRPORT
312 782 1448 ILLINOIS BELL
312 852 0506 HINSDALE SAVINGS
312 852 1305 HEATH
312 852 2899 IBM
312 854 0066 GOOGOLPLEX
312 870 5844 "EARS"
312 922 4531 REROX
312 937 1210 ABBOTT LABS
312 938 0600 MCDONALDS
312 939 8308 DEPAUL
312 960 8670 COSMOS
312 972 7603 ARROGON
312 996 5100 UNIV. OF ILLINOIS
313 234 5621 FTS (FEDERAL TEL)
313 262 6011 TRAVELNET QUESTIONS
313 377 4300 OAKLAND SCHOOL
313 556 1300 TRAVELNET CUST SERV
313 556 4706 TRAVELNET INFO TAPE
313 552 1305 PBX
313 644 3840 HIGH SCHOOL
313 644 3950 ISS
313 769 8821 ANN ARBOR SCHOOL
313 839 3373 MICHIGAN BELL
313 857 5500 OAKLAND SCHOOL
313 857 9506 IBM
313 881 0559 MICHIGAN BELL
313 992 0050 MICHIGAN BELL
313 924 9977 MICHIGAN BELL

by nynex phreak

313 961 8572 MICHIGAN BELL
313 962 7071 BONDNET
313 964 0042 MICHIGAN BELL
313 964 2018 CHARGE CARD ASSOC
313 964 4342 MICHIGAN BELL
313 964 5808 MICHIGAN NAT PARK
313 964 5858 BANK OF DETROIT
314 232 5390 MCDONNELL DOUGLASS
314 231 4510 FORD
314 532 3545 ROOSEVELT FEDERAL
314 569 2286
314 569 6910
315 423 1313 SYRACUSE UNIV
319 386 8850 HP 2000
319 386 8851 HP 2000
402 378 7040 RSTS
404 396 0631
404 424 7563
404 855 3460 SEARS
404 873 8555 CONFERENCE BRIDGE
404 873 8682 AT&T
404 885 3460 SEARS
405 789 2323 BANK OF BETHANY
408 280 1901 TRW
409 845 6203
412 527 8291 FBI
412 794 7661 SLIPPERY ROCK UNIV
414 271 7827 AGRIDA
414 332 3567
414 445 4050 DEC VAX
414 476 8010 DEC
415 327 5229 ARPANET
415 361 2500 MENLO PARK
415 442 2161 AT&T
415 486 4359 DEVELCON
415 495 4294
415 626 4458 NAZI NEWSLINE
415 786 0129
415 788 0662
415 786 1533
415 829 6068
415 857 8193 HP 3000
415 863 9059
419 325 2191
502 454 5824 GENERAL ELECTRIC
503 645 9654
503 963 8454
504 522 5633 BANK OF LOUISIANA
505 623 9280
505 843 9166
509 535 1363
512 474 5081 AUSTIN COMPUTERS
515 294 9449 ISD
516 567 8013 LIRICS
516 632 8900 SUNY MODEM POOL
516 751 2500 2600 MAGAZINE
518 220 6603 RPI
602 965 2001 ARIZONA STATE
603 643 6310 DARTMOUTH
609 452 6736 PRINCETON UNIV
609 645 0533 FBI
612 322 2431 FREEDOM NET
612 332 1737 CTRL DATA TLX
612 393 1567 WESTERN UNION
612 338 5200 INTERNATIONAL GRAPH
612 376 7730 SOFTWARE
616 628 4699
617 258 6251 MIT
617 258 6511 MIT
617 258 6629 MIT
617 258 7115 MIT
617 258 7542 MIT
617 258 8260 MIT
617 258 8313 MIT UNIVERSITY
617 338 5071 USOS BOSTON
617 459 0159 LOWELL
617 471 9203 NORTHEAST UNIV
617 732 0251 HARVARD UNIVERSITY
617 732 1802 HARVARD UNIVERSITY
617 861 5551 HANSCOM BASE
619 225 1641 NATIONAL DEFENSE
619 225 6946 SAN DIEGO
619 236 7884 SAN DIEGO
619 293 4510 UCSD
619 236 5010 COLDWELL BANKER
619 326 2174
619 452 6732 UCSD
619 723 6956 NAZI BBS
701 477 6442 ROLLA COLLEGE
702 329 3559
702 737 8770
703 274 5302 NATIONAL DEFENSE
703 328 8086 VIRGINIA UNIVERSITY
703 781 4520 MERADCOM
703 790 1740 FAA
704 253 0126
704 253 6370
713 483 2700 NASA
713 792 7200 EDUCATION
713 795 1200 SHELL VULCAN
713 868 6499 PBX
713 941 7619 NAZI BBS
714 535 6467
714 987 5552 NAZI NEWSLINE
714 962 3365 HATS
715 232 3688 RSTS
716 467 3242
717 872 0311 MILLERSVILLE UNIVAC
718 276 9775 COSMOS
718 539 3560
718 963 3173 MCI (ZAW)
800 222 0555 BANK OF AMERICA
800 223 2838
800 223 3312 CITIBANK
800 225 8456 AUTONET
800 228 0003
800 228 0018
800 228 1111 CREDIT CHECK
800 245 6216
800 323 0084
800 323 0122
800 323 0170
800 323 0664
800 323 0679
800 325 4112 EASYLINK
800 325 6397
800 325 7222 MCI
800 327 6245
800 327 7725
800 327 9488 ITT TONE
800 327 9538 EASYNET
800 329 0404
800 336 0149 TYMNET
800 336 0437 TELENET
800 358 2711
800 369 3313 THE SOURCE
800 358 9407
800 358 9408
800 358 9409
800 358 9410
800 358 9426
800 392 5149
800 421 2626
800 424 9494 TELENET
800 426 2500
800 426 5151
800 522 5465 LABLINK
800 525 3714 RCA GEORGIA
800 527 1800 BANK BY PHONE
800 533 0092 MESSAGE RELAY
800 633 1538 MOBILE MARINE RADIO
800 637 0959
800 642 1902 EDUCATION BBS
800 821 5662
800 852 2345 PBX
800 852 2255 PBX
800 932 6245
804 865 4051 NASA
805 497 0340 TRW

(continued on page 11)

the telecom informer

BY GOLDSTEIN

All is not well in the home shopping industry. Yes, those ridiculous shop-at-home programs that have been popping up on nearly every television station in the country (including some PBS stations!) are having major problems with their phones. Take Home Shopping Network—the first and biggest of them all. They say more than half of their incoming calls went unanswered last year! So they replaced their old Centrex equipment with a Rockwell International Corporation Galaxy ACD switching system. AT&T provides the switching equipment, so the local central office is completely bypassed. Will it screw up? Stay tuned....The Federal Communications Commission has decided that it's not necessary for cellular phones to be equipped with labels warning that conversations on them can be easily intercepted by anyone with the proper radio. After all, it's now illegal to listen! Brilliant, just brilliant....Perception Technology Corporation is selling equipment to dozens of college campuses that allow students to register for courses using touch tone phones. The two latest are the University of Alaska and Contra Costa Community College of Martinez, California. The equipment is called VO-COM, a descrambling box that links phone lines to the university mainframe computer using a voice response system. Other campuses using similar systems are Lane Community College of Eugene, Oregon; Brigham Young University of Provo, Utah; Louisiana State University at Baton Rouge; the University of Alberta; and the University of Southern California at Los Angeles....MCI hackers, beware! MCI has recently bought the Real Time Toll Fraud Detection System from Applied Computing Devices Inc. of Terre Haute, Indiana. The system uses on-site selection and compression of call data for rapid detection of toll fraud. The system uses a network of ACD's Universal Billing Converters and Interface Adaptor Units to monitor remote sites using the UBX Network Call Data/Billing Data Management System....Pacific Bell is in trouble. Someone called the Suicide Prevention Center in Burlingame, California threatening suicide. A center representative asked PacBell to trace the number and PacBell cheerfully gave the wrong address. A woman who happened to live at the wrong address said rifle-carrying police officers and a large black attack dog came charging through her apartment. (Suicide is illegal, you know.) She's suing PacBell for alleged invasion of privacy as well as physical and emotional damages. In all the fun, no one seems to know what happened to the original caller....Did you know that the most prestigious exchanges in the Hamptons are 324 (East Hampton) and 283 (Southampton). The nouveau-riche must settle for 329 (East Hampton) and 287 (Southampton). New York Telephone reps say they've been offered bribes for numbers with the old exchanges. Some status-conscious people have been using answering services inside the old exchanges to avoid being embarrassed. More practical types are furious over the fact that call-waiting and equal access aren't available (every one of the exchanges is crossbar)....Cockroaches, fire ants, and wasps are the most common insects found in phone equipment and they can cause extensive damage, according to South Central Bell officials. "Spiders spinning webs across terminals cause moisture to collect on a terminal, leading to shorting out or glitches in your telephone connection," an official said. "Termites can actually bore through cable lines." We've decided not to print any phone bugging jokes here, sorry....Of the $64.2 million collected by

(continued on page 21)

FBI revealed

The FBI Project Newsletter
The FBI and Your BBS
Published by Glen L. Roberts
Box 8275-N1
Ann Arbor, MI 48017

Review by Emmanuel Goldstein

Two very important and relevant publications came our way recently, both published by the *Full Disclosure* folks. They concern the Federal Bureau of Investigation and they will prove intriguing to many. *The FBI Project Newsletter* is a quarterly newsletter that promises to keep readers up to date on FBI abuses and activities. *The FBI and Your BBS* is a must for anyone interested in running a computer bulletin board system.

Included in both publications is a history of the FBI, illustrating how the original intentions of the agency have become tarnished over the years. Some instances of abuses include cover-ups of criminal acts by agents and informants, violations of the Privacy Act, and surveillance and searches of political activists.

"The best measurement," according to the newsletter, "of the FBI's activities was done on March 8th, 1971, when all the records were stolen from the FBI's office in Media, PA. They show that the FBI's active cases at that time were broken down as follows: 40% political surveillance and other investigation of political activity (2 right wing cases, 10 immigrants cases, and over 200 left wing cases); 25% murder, rape, and interstate theft; 7% draft resistance; 7% leaving military without permission; and 1% organized crime (mostly gambling)."

We don't know what happened to the other 20% and we can't really vouch for the accuracy of these figures. But we do know that things are going on in the FBI that have quite a lot of people up in arms, and computer users are no exception. The newsletter gives tips on how to find out what the FBI is doing in your area—everything from listening to their radio frequencies to staking out their hangouts and doing some surveillance of your own.

The FBI and Your BBS provides advice on protecting your bulletin board system from FBI snooping. By making a system private, it becomes a crime for an FBI agent (or anyone else) to use the system without authorization. This is true due to our old friend, The Electronic Communications Privacy Act. Using the ECPA in this way is indeed ironic, but as the newsletter says, we must "do our best to make sure the government follows its own rules."

We like the spirit of this newsletter and we think anyone interested in either the FBI or computer bulletin boards will find much worthwhile reading here. For the future, we hope to see more references to other kinds of law enforcement entities, such as our friends, the Secret Service. Limiting the subject matter to only one organization will be somewhat restrictive and might lead some to believe that the publishers have a vendetta against the FBI, even though it is unquestionably the most visible of these agencies. We also hope to see the ideas and values presented here show up on bulletin boards across the country. Mass awareness is really the only way to get these facts out.

To subscribe to this newsletter, send $10 to The FBI Project, Box 8275, Ann Arbor, MI 48107. Send $5 for a copy of *The FBI and Your BBS*.

CAPTURING PASSWORDS

by Texas Toad

Many times if you are already a user on a VAX VMS system, it would be handy to have the account names and passwords of other users of the system. In order to get additional names and passwords, I wrote the DCL (DEC Control Language) command file below which will simulate the normal login screen on a VT100 or compatible terminal, and will write the user's account name and password to a file in your account, and will then abort as if a line glitch had occurred.

The user who enters his name and password should not be suspicious, since the login appears to abort from natural causes. In the event that he/she is, however, the CTRL B TAB command sequence defined will force an exit from the network or host system before control is passed back to the user. Note that the CTRL B TAB sequence is system-specific and should be whatever characters are used on your system to disconnect the terminal or process from the host computer.

The files USER.TST and PASS.TST contain the user's login name and password, respectively.

Another handy trick is shown below. This command creates a file in your account which will subsequently capture *all* the activity occurring at your terminal. *Any* keystrokes, *any* commands, all the actions done at the keyboard will be logged in the file as well as going on at the terminal as normal.

SET HOST/LOG=filename 0

Be sure to include a legal VMS filename and be sure to include the zero following the filename.

Once the user or whoever logs off, system control returns to the account from which the above command was given. At that point, the filename specified now has the contents of the session. It may be necessary, if you want to edit the file with EDT or a standard text file editor, to run the following command:

MCR REF

This will convert non-ASCII control sequences (like terminal control characters) to spelled-out ASCII codes (like ESC for the Escape key). The file can then be examined at will.

Interested in more VAX goodies? Have terminal will travel.

USE THESE IF YOU ARE CONNECTED BY A LAN TO YOUR VAX

```
$ SET NOCONTROL_Y
$ INQUIRE/NOPUNCTUATION RETURN "2J"
$ TYPE SYS$INPUT
You may now enter Net/One commands
$ INQUIRE/NOPUNCTUATION GREATER ">"
$ TYPE SYS$INPUT
connecting...(1) 1616956 success
$ INQUIRE/NOPUNCTUATION NULL ""
$ WRITE SYS$OUTPUT "2J"
$ WRITE SYS$OUTPUT "10,0H"
$ TYPE SYS$INPUT
```

THIS IS WHERE YOUR PARTICULAR LOGIN MESSAGE GOES

```
$ INQUIRE Username "Username"
$ SET TERM/NOECHO
$ INQUIRE Password "Password"
$ OPEN/WRITE OUTFILE PASS.TST
$ WRITE OUTFILE Password
$ CLOSE OUTFILE
$ OPEN/WRITE OUTER USER.TST
$ WRITE OUTER USERNAME
$ CLOSE OUTER
$ TYPE SYS$INPUT
User authorization failure
$ ! WAIT 00:00:05
$ CTRL_B[0,7] = %X0002
$ TAB[0,7] = %X0011
$ CTRL_B_TAB = CTRL_B + TAB
$ WRITE SYS$OUTPUT CTRL_B_TAB
$ EXIT
```

PASS.TST WILL CONTAIN THE PASSWORD OF USER

USER.TST WILL CONTAIN THE NAME OF USER

numbers

(continued from page 7)

```
805 497 5393 IBM
805 497 6832 MAY CORPORATION
805 527 7213
805 765 7605
806 353 9901 CIA
808 477 5844 CAMP H.M. SMITH
809 477 6833 CAMP H.M. SMITH
808 477 6839 CAMP H.M. SMITH
808 477 6843 CAMP H.M. SMITH
808 477 6946 CAMP H.M. SMITH
808 488 6227 CAMP H.M. SMITH
815 729 0586 JOLIET COLLEGE
816 471 1939 METRO TONE
816 842 0030 FBI
816 842 0051 FBI
816 842 1870 LOG TIME
817 332 8481 FT WORTH SCHOOL
817 625 6101 GIS
818 885 0473
818 358 7356 NAZI NEWSLINE
904 882 3242 ELGIN BASE
904 882 3246 ELGIN BASE
904 882 8201 ELGIN BASE
904 882 8202 ELGIN BASE
912 926 2204 ROBINS AIR FORCE
912 926 2725 ROBINS AIR FORCE
912 926 3231 ROBINS AIR FORCE
912 926 3232 ROBINS AIR FORCE
912 926 9725 ROBINS AIR FORCE
914 257 4201 SUNY
914 347 5540 BOCES
914 471 4853 MARIST COLLEGE
914 623 0402 MANUFACTURERS NATIONAL BANK
916 324 5915 ARYAN NATIONS HOTLINE
918 258 4847
```


at&t sub maps

by Bernie S.

Finally, something free from AT&T! I've just received two copies of the "Submarine Cable Systems Chart of the World," a beautiful 38" x 52" seven-color map produced by the International Cable Engineering Department of AT&T's Long Lines Division.

I first became aware of this map last summer when a friend showed me a key ring an AT&T engineer had given him. It said, "Free AT&T Submarine Cable Maps" and listed a phone number. When I called it, the woman who answered knew nothing about maps but suggested another AT&T number to try. After five more calls like this, I finally reached AT&T's International Engineering Division. The man there denied that such maps were available, but after a little "social engineering" (I told him I was a university professor of telecom engineering and needed the map as a teaching aid), he conceded that a new version was being readied and that he'd see to it that I got a copy. Four months later the maps arrived in a big tube—it was worth the wait.

The map, a mercator projection dated December 1986, shows in surprising detail present and proposed submarine cables color-coded as AT&T's, others, and lightguides. To the best of my knowledge, no major transoceanic optical fibers have been laid yet, but this map shows them anyway. A disclaimer states, "NOTE: Chart scale prohibits the display of all submarine cable systems. Precise political and geographic distinctions are not within the scope of this representation." Still, the map shows quite a lot and is a respectable world map in its own right. In addition to submarine cable systems, the map details and labels all significant land masses, ice shelves, ocean depths and trenches, mountain ranges, political boundaries, and latitude and longitude.

The Submarine Cable Systems Chart of the World will look great on any hacker's or phreaker's wall. It obviously cost AT&T a lot of money to produce, so they'll probably be reluctant to give them away to just anybody. Be sure you have a plausible story cooked up as to why you deserve a map before demanding one. Good luck!

here are the letters

CNA/CPA Questions

Dear *2600*:

I don't understand your listing of CNA (Customer's Name and Address) numbers. For instance, my area code is 305 in Florida. According to your listing, I have to dial area code 912 (7840440) to get a customer's name and address. This seems strange because area code 912 is located in the State of Georgia and I have to pay a toll charge if I use this area code.

I have Radio Shack's Duophone CPA-1000. If all "pen registers" work the same as this one, they can be easily voided. The pen register will not record the number of an outgoing call if same is made on a cordless telephone. The call is listed as an incoming call without the telephone number.

If anyone has a suspicion that spies are registering his outgoing call numbers they have only to use the cordless phones, without worrying that same are being recorded.

No mention was made of this in your article "A Pen Register For Phreaks" in your last issue, or didn't you have any knowledge of this?

Samuel Rubin

If you take a look at our CNA list, you'll see that many area codes have their CNA bureaus located somewhere else, often in other states. It's one of those bitter ironies we hear so much about.

It's quite true that the pen register can be fooled into thinking that a cordless call is really an incoming call. We're not sure if all pen registers can be tricked this easily. However, keep in mind that when you use a cordless phone, you're broadcasting your conversation over the radio, which can be quite damaging. If this works consistently, the best method would be to dial on a cordless phone and then transfer to a regular phone. Unless of course, you're being tapped. A face to face conversation in the middle of a huge empty parking lot might be the answer. But then there are satellites...

ITT Switching

Dear *2600*:

The letter from Bernie S. in the May issue parallels my experience with an ITT 2100 switch I was responsible for in my old office. That office has been closed down for a year, and I didn't copy the documentation, so I can only describe it in general terms—but here goes.

We were a software development team located in Bergen County, NJ. In addition to the usual complement of local service (NJ Bell) lines, our office had 2 sets of lines for inward-WATS service (New Jersey and New York), and 2 sets of lines for outward-WATS (for New Jersey and the rest of the country—Band 5). What the ITT switch provided was called DISA, "Direct Inward System Access". If you called in on certain numbers in any of the sets, it bypassed the receptionist's board and got a dial tone, just as though you had picked up a phone on the premises. You could then dial an office extension directly, dial 9 for an outside (local) line, or—drum roll, please!—dial 81 or 82 to get an outside WATS line.

This switch was also programmable—the assignment of what number(s) to dial for an outside line; assign "hunt groups" (make calls to a busy number "hunt" another phone to ring); special features of multi-button phones (each button was programmable to perform any available function); assign a pecking order of numbers that could interrupt calls on other extensions, etc., etc. There was a provision for numeric passwords for the WATS lines, but we never implemented it.

The entire system was basically a giant table of what internal line had what kind of phone and its privileges. The table was kept in both RAM and non-volatile memory: when you were satisfied with your changes, you told the switch to save them. Programming was done through a serial port, which was hooked up to a 300-baud modem. Since this modem was on the phone system, this meant that it was accessible to the outside world (ITT Customer Support, by intention, but also the world generally) by calling in on a designated DISA line. Usually, however, ITT service people visiting the site would bring a custom mini-terminal or a Radio Shack Model 100 with them and hook up directly to the serial port. The system was password protected, but the default "master" password is pretty obvious.

The original idea was that us programmer types could have terminals at home, and if we got called to take care of a client's blowup, we would call in to work (on a local number if we lived close enough, or on the in-WATS if further out) and dial up the client machine on the out-WATS. In practice, it never worked worth a damn because the end-to-end line losses involved in going from WATS to WATS prevented our cheap modems from handshaking.

The powers that be lost interest in the system when it became apparent that (A) it wouldn't provide the work-from-home capability they were promised, and (B) the bozo employees couldn't keep straight when to use in-WATS and when to call in on their own nickel. (Least-cost routing was a pretty far-out concept for most of them. Of course, if some of them were using the system to call Mom in Palm Springs, it wouldn't have shown on the WATS bill, which gave only total hours of use. Is *that* why WATS lines are cheaper than regular ones?)

Oh, by the way—I tried the Carolina Beachcomber's VAX program under an account that has CMKRNL but NOT CMEXEC; it works under that situation, too. Gives a fella a warm fuzzy feeling just to know that it's there if he really *needs* it...

The Primal Wombat

Hotline Numbers

Dear *2600*:

My mailbox is always full of mail promoting some kind of Investment Advisory Service. These services tell you all about the economy, where it's headed, and what to invest in to make big bucks. For a fee (ranging from $19 to $149) these services mail out a monthly newsletter recommending the hottest stocks, bonds, funds, options, all kinds of things.

Most of these services also provide a telephone hotline to call for daily or weekly advice, while waiting for the newsletter.

If any of your readers know of any of these phone numbers, how about publishing the list? Who knows, we might all get rich (legally) while we read *2600*!

Frank B.

Monitoring Cellular

Dear *2600*:

Updating the information contained in the "Telecom Informer" of your April issue:

The 800 mhz mod diode was moved from the underside of controller board PC-3 in later models of the Radio Shack Pro-2004 scanner. Snipping one end of the diode is still the modification, however. One almost gets the feeling that Radio Shack wanted to make it easier for us to monitor cellular telephones.

(continued on page 18)

The Summer Games of 1987

(continued from page 5)

you're saying so there's no misunderstanding. Avoid local TV news—they're mostly after ratings.

Naturally, you should try not to let yourself get into a situation where such unpleasant things can happen to you. But sometimes that isn't enough. In 1985, The Private Sector, a bulletin board run by 2600, was seized merely because its phone number had been mentioned on another bulletin board system that was being investigated. Clearly, these are precarious times.

On the subject of bulletin boards, we've made some important decisions in the last month. We are going to try and start up some boards as quickly as possible. Each of our boards will have public levels that are open to anyone who calls in. Verification of callers will not be required. Being anonymous is your right. Each caller will also be given a private mailbox, through which he can communicate with other individual callers. What goes on in the private mailboxes will only be seen by the sender and the receiver. The system operator won't even be able to access this information, at least not without resetting the account so the password no longer works. Passwords will also not be accessible by anyone other than the caller.

We feel this will uncloud the issue of what is legal and what is not. On the public levels, illegal information, such as credit card numbers and long distance codes, won't be permitted and will be removed if spotted. Public levels will be accessible to everyone who calls. Private mail will remain private. It will be analogous to the mail we get from the post office. By making these distinctions, we think it will become much harder for bulletin boards to be "raided" because of supposedly illegal activities.

We've received some calls from folks interested in running bulletin boards. We now need software that can perform the above functions. If you have access to this, please contact us.

If you belong to a company or organization that agrees with what we're saying, you might want to donate or loan computer equipment for this purpose. We'll also be happy to run boards for anyone who wants to sponsor one, but has misgivings about doing it from their home. We have the means to save a little bit of freedom here. We cannot do this alone.

2600 HAS MEETINGS

Every Friday afternoon
between the hours of 5 and 8
in the Market area of the Citicorp Center
in New York City,
53rd Street and 3rd Avenue

A HACKER SURVEY

At times like these, people begin asking philosophical questions. What is right and what isn't? We thought that would be a good subject to ponder for the hackers of the world and this is what we've managed to come up with so far. Feel free to write in with your own comments, whether you're a hacker or not.

The one thing that most of the hackers we spoke with seem to agree upon is that stealing merchandise with credit card numbers is wrong. Many went on to say that this does not comprise hacking at all. In other words, any moron can get a credit card number and many do.

Why are such people categorized as computer hackers? Probably because some of them use computers to get credit card numbers, said a few. Others believe it's because the public and the media don't understand how anything involving credit card fraud can be accomplished without the help of a computer. It's quite possible to commit credit card fraud simply by picking a credit slip out of the garbage or by standing around an ATM machine until somebody discards a receipt that has their Visa number on it. Since many credit checks don't verify the person's name or the card's expiration date, it's become extraordinarily easy. Which is another reason many hackers dislike it.

What should happen to such people? Many hackers believed they should be dealt with severely, although prison terms weren't mentioned. Almost all believe they should pay back whatever it was they stole.

How about long distance fraud? Reactions to this were mixed. Some feel that ripping off long distance companies is exactly like credit card fraud. Others believe it's a few steps above it, particularly if a hacker uses ingenuity and common sense to avoid being caught. A few questioned whether or not there was actually any loss of money to the company involved, particularly the big ones. "Who does AT&T have to pay when they're stuck with a fraudulent phone bill? Do they pay themselves? The smaller companies usually pay AT&T, but who do the bigger companies have to pay? It's not like we'd make a two-hour call across the country if we had to pay for it, so the lost revenue speech is kind of hard to swallow." "It seems to me that the phone lines would still be there whether or not we were on them, the computers would still be running if we weren't on them, either way the cost to the company is almost the same." A few pointed out that the bad publicity surrounding code abuse probably does more harm than the actual phone bills.

Some said that toll fraud was a necessary part of computer hacking, but it wasn't a form of hacking in itself. But nearly all we questioned seemed to agree that when caught, the culprit should be made to pay back what they used, as long as they're presented with evidence that they made the calls.

What kind of hacking is acceptable in the hacker world? Generally, access to systems that a hacker would never gain access to, regardless of how much he was willing to pay. Systems like the phone company computers, credit checks, census bureaus, and private military systems were mentioned most. "By accessing these, we're learning a lot more than we ever could on Compuserve." "We can uncover lots of secrets, like how easy it is to change somebody's credit or how easy it is to find an unlisted phone number. People would never know these things if it weren't for us." These kind of hackers look upon themselves as "technological Louis and Clarks".

What kind of price should a hacker pay if he's caught on a non-public system? A few said a fine of some sort should be imposed. But most seemed to believe that an agreement of some sort could be reached between the various parties, such as the hacker telling the operators how they accessed their system and what bugs

(continued on page 22)

Telenet
A US Sprint Company

Telenet Communications Corporation
12490 Sunrise Valley Drive
Reston, VA 22096
703 476-1040

7/01/87

Dear PC Pursuit Customer:

You may be aware of the FCC's recent proposal to impose switched access charges on Telenet and the other enhanced service providers (ESPs). This letter is being sent to all PC Pursuit users to provide some initial information on the new FCC proposal and to answer questions you may have regarding the proposal and its potential impact on PC Pursuit and other computer-based services.

Switched access charges (also called "carrier access charges") were originally devised by the FCC as the interexchange carriers' means of payment for their use of the local exchange dial network in originating and terminating long distance traffic. Now the FCC proposes to extend these access charges to enhanced services such as Telenet's PC Pursuit, as well as to any other computer-based service which has interstate traffic, including database services, electronic mail, computer conferencing, home banking/shopping, timesharing, and videotex.

Based on information now available from the FCC, we estimate that access charges would add approximately $4.50 per hour to ESP costs for dial-in access to a remote host computer, and $7-9 per hour for a service such as PC Pursuit which uses both dial-in and dial-out access on each call. PC Pursuit customers and other computer users would be particularly affected by these access charges. PC Pursuit's current "Flat-rate/unlimited usage" service would have to be repriced on a per usage basis, incorporating the $7-9 per hour access charge. It is doubtful that the service could survive at this inflated rate.

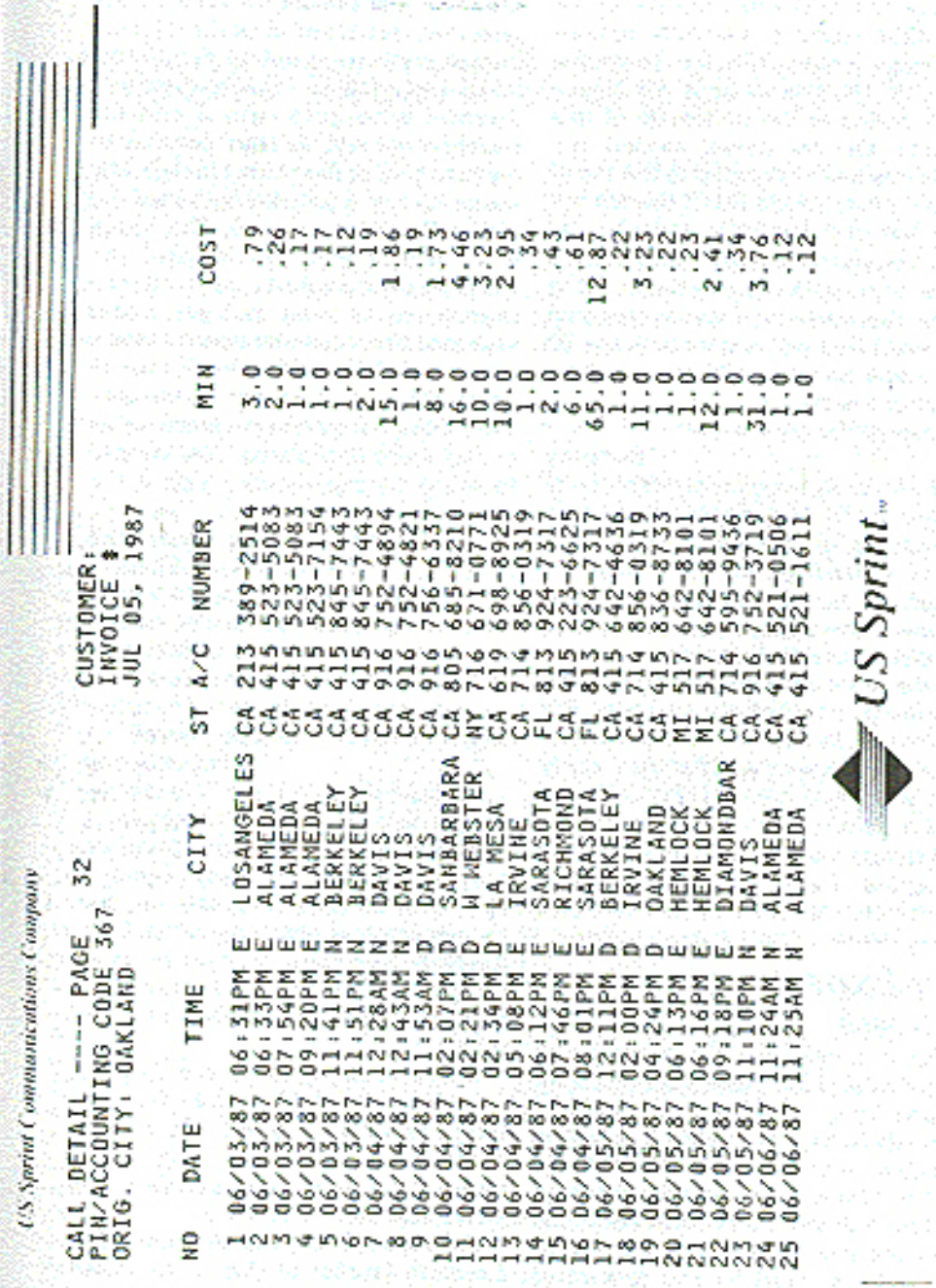
Telenet and the other enhanced service providers intend to fight the FCC's proposal. You can assist in our effort by letting the FCC and your Congressional representatives know how access charges will adversely affect your ability to reach information and remote BBS systems affordably. The FCC has asked for this input. Please use this opportunity to add your voice to the debate and stop the proposed increase.

Once the FCC's official Notice of Proposed Rulemaking has been published, we will provide more details on the proposal. This information will include addresses and other information for your letters, and the FCC's schedule for receiving comments on the proposal. In the meantime, please address your questions or comments to FCC.ISSUES on PC Pursuit's Net Exchange BBS. PC Pursuit customers can access the Net Exchange using the following sign-on procedures:

@C PURSUIT, YOURID (CR)
PASSWORD=YOURPASSWORD (CR)

Working together, we defeated a similar proposal which would have applied access charges to PC Pursuit and other enhanced services just three months ago. With the same effort now we can repeat our victory, and protect the important computing resources we enjoy affordably today.

WE NEVER THOUGHT WE'D SEE THE DAY WHEN THIS MAGAZINE would actually donate space to a huge corporation in order to give them a chance to get a message through. Well, in this particular case, they make a lot of sense. It's a rare occurrence, but it does happen now and then.



US Sprint Communications Company

CALL DETAIL ---- PAGE 32
PIN/ACCOUNTING CODE 367
ORIG. CITY: OAKLAND

CUSTOMER:
INVOICE #
JUL 05, 1987

NO	DATE	TIME		CITY	ST	A/C	NUMBER	MIN	COST
1	06/03/87	06:31PM	E	LOSANGELES	CA	213	389-2514	3.0	.79
2	06/03/87	06:33PM	E	ALAMEDA	CA	415	523-5083	2.0	.26
3	06/03/87	07:54PM	E	ALAMEDA	CA	415	523-5083	1.0	.17
4	06/03/87	09:20PM	E	ALAMEDA	CA	415	523-7154	1.0	.17
5	06/03/87	11:41PM	N	BERKELEY	CA	415	845-7443	1.0	.12
6	06/03/87	11:51PM	N	BERKELEY	CA	415	845-7443	2.0	.19
7	06/04/87	12:28AM	N	DAVIS	CA	916	752-4894	15.0	1.86
8	06/04/87	12:43AM	N	DAVIS	CA	916	752-4821	1.0	.19
9	06/04/87	11:53AM	D	DAVIS	CA	916	756-6337	8.0	1.73
10	06/04/87	02:07PM	D	SANBARBARA	CA	805	685-8210	16.0	4.46
11	06/04/87	02:21PM	D	W WEBSTER	NY	716	671-0771	10.0	3.23
12	06/04/87	02:34PM	D	LA MESA	CA	619	698-8925	10.0	2.95
13	06/04/87	05:08PM	E	IRVINE	CA	714	856-0319	1.0	.34
14	06/04/87	06:12PM	E	SARASOTA	FL	813	924-7317	2.0	.43
15	06/04/87	07:46PM	E	RICHMOND	CA	415	223-6625	6.0	.61
16	06/04/87	08:01PM	E	SARASOTA	FL	813	924-7317	65.0	12.87
17	06/05/87	12:11PM	D	BERKELEY	CA	415	642-4636	1.0	.22
18	06/05/87	02:00PM	D	IRVINE	CA	714	856-0319	11.0	3.22
19	06/05/87	04:24PM	D	OAKLAND	CA	415	836-8733	1.0	.22
20	06/05/87	06:13PM	E	HEMLOCK	MI	517	642-8101	1.0	.23
21	06/05/87	06:16PM	E	HEMLOCK	MI	517	642-8101	12.0	2.41
22	06/05/87	09:18PM	E	DIAMONDBAR	CA	714	595-9436	1.0	.34
23	06/05/87	11:10PM	N	DAVIS	CA	916	752-3719	31.0	3.76
24	06/06/87	11:24AM	N	ALAMEDA	CA	415	521-0506	1.0	.12
25	06/06/87	11:25AM	N	ALAMEDA	CA	415	521-1611	1.0	.12

US Sprint™

NOW THIS IS MORE LIKE IT! A page from the $1200 Sprint bill we got this month! We chatted with them about this last month when we first discovered that the code they never bothered to tell US about had gotten into the wrong hands. "Don't worry," they said. "We'll take care of it." Do we look worried?

letters

(continued from page 13)

To restore 800 mhz coverage on the Pro-2004 scanner, carefully remove the cover and locate the controller board PC-3. Early versions will have a diode added to the underside of this module. On the newer models the diode has been relocated to the top of PC-3. Locate Diode D513 toward the back left of the module and clip one end. (You can remove it entirely, but it's easier to put back together for servicing under the warranty if you simply snip one end.) This will restore both the 30 khz steps and the 800 mhz cellular telephone band.

Keep up the good work!

Stingray

The federal government has recently sided with the cellular phone companies in allowing them to not place warnings on their phones admitting to the possibility of their phone calls being listened to. Our position is simple: listening to a radio is not the same as tapping into a line. For one thing, it's a hell of a lot easier. But there is really no invasion of privacy in receiving something that has come into your own home. Eventually, we feel, the crazy law that makes it a crime to listen to certain frequencies will be repealed. Especially if plans and modifications like the above continue to proliferate. Send us yours today!

An Experience

Dear *2600*:

About a year and a half ago I was apprehended for "unauthorized use of phone lines". Here's my experience in a nutshell. Myself and my friend, The Ice Lord, rang up most of about $8000 worth of fraudulent calls to a small long distance service that couldn't afford to take the loss. Through carelessness, we were busted by the jerkwater sheriff's department in cooperation with some incompetent PI's and the FBI. They fumbled around with my system and gave away the fact that they had just busted Ice Lord by the way they accessed disk directories before packaging up my computer, notes, and joysticks. I would advise that anyone who gets into a similar situation not talk, as I did, because in my case cooperation didn't make it any easier on me. It just strengthened the plaintiff's case anyway. The judge went pretty easy on us and the insurance company settled the lawsuit, so as soon as I get a new keyboard (the cops managed to waste most of my Comm-64's chips), life will get mostly back to normal. By the way, even though they had evidence, other crimes were overlooked. Just wanted to share my experience—hope it's of some value.

I love your mag but can I anticipate something more in the way of how-to articles and beginning to semi-technical projects? Also, I'm looking forward to hearing about a 2600 meet on the west coast. Any chance of it?

Lastly, can you give me the full story on Bill Landreth's disappearance?

The Sorcerer

We hope when you say "life will get back to normal", you don't mean you'll continue to openly commit fraud on some poor phone company. There is very little of what you told us that sounds like true phreaking or hacking. Anybody can make free phone calls these days but only a few know how to thoroughly explore and discover new tricks.

We're looking for more how-to articles which our readers are encouraged to submit. As far as meeting on the west coast, that depends on how many people seem interested.

We don't know much about Bill Landreth (author of Out of the Inner Circle), but word has it that he's reappeared.

(continued on page 22)

2600 marketplace

A FULL PAGE AD in 2600 costs only $200. Half page, $100. Contact 2600 Advertising, PO Box 762, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

FOR SALE: COMMODORE 8-BIT ROBOTICS KIT by Fischertechnik. All hardware, interface, software and manuals included. Mint condition. $399. Send phone # to: Box 571, Forest Hills, NY 11375.

WANTED DESPERATELY: High-speed shredder capable of handling hardcover documents. Contact 2600 Magazine ASAP. 516-751-2600. Ask for Rocco.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochelis. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100.00. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

***2600* MEETINGS.** Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label.

Deadline for September issue: 9/5/87.

(continued from page 18)

Phone Literacy

Dear *2600*:

Your readers might be interested in knowing about a publication devoted to exposing federal surveillance: Full Disclosure, $15 from Box 8275, Ann Arbor, MI 48107. Also, for an early example of phone phreaking, check out Philip Agee's spellbinding new book, *On the Run*. As the CIA was hounding Agee from country to country, it was essential for him to stay in touch with his international network, which he did partly through "express phones" around Paris which had had a small slot drilled above the coin counter into which a paper clip could be inserted.

Finally, a comment on Izzy Hear's letter in the May issue. Like Izzy, I know electronics and am computer-literate, but a lot of the specialized language in the world of phone-tech leaves me baffled. How about if *2600* puts together a special issue some time devoted to bringing your less-sophisticated readers up to speed? I'd especially like to see a good list of manuals that could lead one from more elementary to more advanced understanding.

I think we agree that in coming years phone literacy is going to be as important for resisting the police state as computer literacy. One example is the British disarmament movement, CND, whose members have been fighting a running battle for years over malfunctions that always seem to happen to their heavily tapped phones at crucial moments. Another concerns the fall of Allende in 1973: in the early hours of the fateful morning as Pinochet's tanks began rolling towards the Presidential Palace, it appeared that the phones of about 2500 of Allende's closest associates in government had gone dead. In his book on the Allende "destabilization", the US ambassador at the time marvels that this could have been accomplished in a few hours by only two phone technicians. Gee, GTE? No, ITT.

Audie O'Sirkit

We never did trust them anyway.

WRITE A LETTER!

And send it to us!

If you have questions or comments about our magazine or about computer hacking and phone phreaking, write them down and send them to

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

SURVEY

(continued from page 15)

were present to allow them to do this. Very few were sympathetic to companies or organizations that allowed hacking to go on for long periods of time. "It's their own fault—who else is there to blame? If we didn't get in there, somebody else would have." "Lots of times we tell them about their bugs, and they either ignore us or just fix it without even saying thanks. I think they deserve what they get, honestly."

Hackers have a distinct definition of what is good hacking and what is bad hacking. Bad hacking would include actions like crashing a system for no particular reason. "Good hacking is entering a system, creating ambiguous accounts, covering your tracks, defeating the accounting, gaining high access, exploring, learning, and leaving. A bad hacker erases files and reads others' mail."